REVIEW OF COMPUTER ENGINEERING STUDIES

ISSN: 2369-0755 (Print), 2369-0763 (Online)
Vol. 4, No. 2, June 2017, pp. 76-81
DOI: 10.18280/rces.040207

A publication of IIETA

IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering
http://www.iieta.org/Journals/RCES

Cloud computing: its characteristics, security issues and challenges

Achla Gupta, Soma Bandyopadhyay*, S.S. Thakur

Computer Science and Engineering, MCKV Institute of Engineering, Liluah, Howrah 711204, India

Email: somabanmuk@yahoo.co.in

ABSTRACT

With the advent of Internet technology, cloud computing has become backbone for IT enabled serviceswith tremendous momentum. It is a growing paradigm which offers on-demand services on a pay-per-use basis. Now a days the need for online services such as storage space, software, platforms etc. is increasing rapidly. Cloud computing is a model for enabling on-demand, on-network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services). Due to its virtualization technique, location independency, scalability cloud has revolutionized IT and business regime in today's era. This paper aims to provide basic understanding of cloud, the technological innovation regarding this field, its service and architecture in a brief and lucid manner. In addition to that the advantages, different security issues and challenges in cloud computing have been highlighted in this paper.

Keywords: Cloud Computing, Internet Technology, Cloud Architecture, Services, Security.

1. INTRODUCTION

Cloud computing is increasing at a brisk pace with the advancement of modern society. Cloud is a network of networks which provides remote access to a set of decentralized IT resources. The term network cloud or cloud was introduced in the early 1990s throughout the networking industry. It referred to an abstraction layer derived in the delivery methods of data across various heterogeneous public and also semi-public networks that were primarily packet-switched. The networking method at this point supported by the transmission of data from one end-point (local network) to the Cloud (wide area network) and then further decomposed to another end-point. Since 2000, cloud computing has come into existence. In early 2008, NASA's Open Nebula became the first open-source software for deploying private and hybrid clouds, and for the federation of clouds. By mid-2008, Gartner saw an opportunity for cloud computing to shape the relationship among consumers of IT services, those who use IT services and those who sell them and observed that organizations are switching from company-owned hardware and software assets to per-user service-based models so that the projected shift to computing will result in dramatic growth in IT products in some areas and significant reductions in other areas. In August 2006 Amazon introduced its Elastic Compute Cloud [1]. Microsoft Azure was announced as "Azure" in October 2008 and was released on 1st February 2010 as Windows Azure, before being renamed to Microsoft Azure on 25th March 2014 [2]. For a time, Azure was on the TOP500 supercomputer list, before it dropped off it [1]. In July 2010, Rackspace Hosting and NASA jointly launched an open-source cloud-software initiative known as OpenStack. On 1st March, 2011 IBM announced the IBM smart cloud framework to support smarter planet [2]. Among the various components of the Smarter Computing foundation, cloud computing is a critical part. On 7th June, 2012 Oracle announced the Oracle Cloud [2]. While aspects of the Oracle Cloud are still in development, this cloud offering is poised to be the first to provide users with access to an integrated set of IT solutions, including the Applications (SaaS), Platform (PaaS), and Infrastructure (IaaS) layers [3, 4]. Nowadays cloud computing comes with on demand self-service, broad network access, resource pooling, rapid elasticity and measured service. This is the first reason to choose the cloud environment, on demand remote capacity with least of organizational effort and minimum interaction of the customer with the service-provider. By improving the storage and data handling capability and bringing down processing time cloud has become a highly demanded service or utility. To cater to this growing market, the infrastructure and number of service providers are also increasing. Middleware controls the entire communication of cloud network which results in security issues. In this work cloud architecture is described in section 2, different services are discussed in section 3. Section 4 focuses on the advantages of cloud computing along with different security issues and challenges in section 5, followed by the conclusion.

2. CLOUD ARCHITECTURE

The cloud infrastructure framework consists of the following components [5]:

- Physical infrastructure
- Virtual infrastructure
- Applications and platform software
- Cloud infrastructure management tools

The resources of the above components are aggregated to provide cloud services. Figure 1 shows cloud architecture.

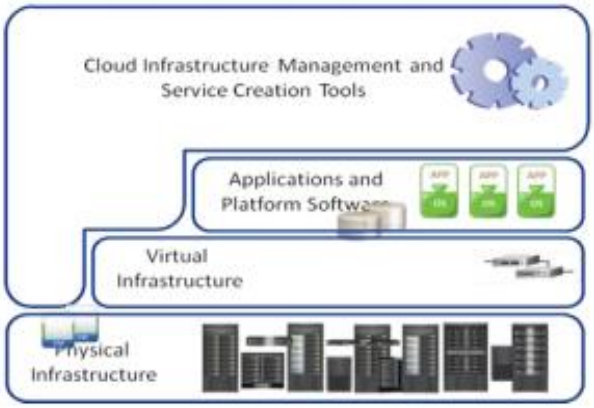

Figure 1. Cloud architecture

2.1 Physical infrastructure

The physical infrastructure consists of physical IT resources which include physical servers, storage systems and physical network components such as physical adapters, switches and routers. Physical servers are connected to each other and to the clients via physical networks such as IP network, FC SAN, IP SAN, or FCoE network.

2.2 Virtual infrastructure

Virtual IT resources consist of virtual machines (VMs), virtual volumes, and virtual networks. VM network components such as virtual switches and virtual network interface cards (NICs).

2.3 Applications and platform software

Applications and platform software layers include a suite of software such as:

- Business applications
- Operating systems and database.
- Migration tools

Applications and platform software are hosted on VMs to create Software-as-a-Service (SaaS) and Platform-as-a-Service (PaaS).

2.4 Cloud infrastructure management and service creation tools

Cloud infrastructure management and service creation tools are responsible for managing physical and virtual infrastructures. They enable consumers to request for cloud services; they provide cloud services based on consumer requests, requirements and allow consumers to use their services.

3. CLOUD SERVICES

The three service models which are recognized by the cloud computing definition of National Institute of Standards and Technology (NIST) are SaaS, PaaS, and IaaS [6]. It is very crucial that we contemplate the importance of considering the impact of cloud service models and their different issues while talking about the security design and implementation. SaaS provides users with a great accessibility of cloud services using a network connection, normally over the internet and through a normal web browser. There has been an emphasis on web browser security while considering SaaS cloud system security. Cloud consumers of IaaS are provided with virtual machines (VMs) that are executed on hypervisors on the hosts, therefore super-quality of security for achieving VM isolation has been studied extensively for IaaS cloud providers who use virtualization technologies. In this section we will discuss about these three different service models. Figure 2 shows the cloud service model.

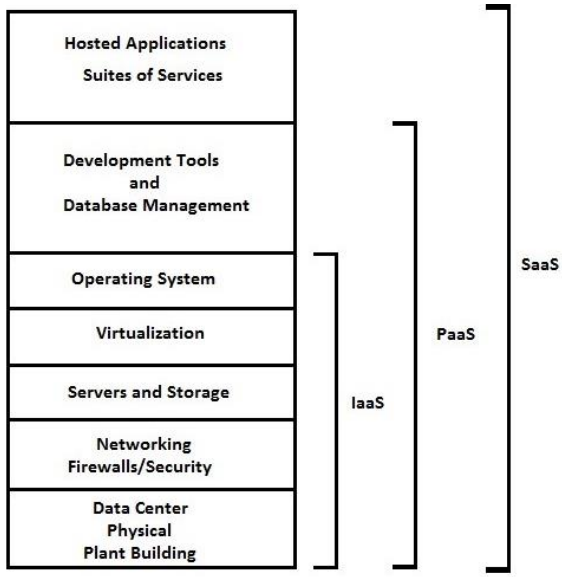

Figure 2. Cloud service model

3.1 Software as a Service (SaaS)

In this model, customer gets complete application on demand. Multiple end users can avail the service when a single instance of the service runs on the cloud. Customers do not need any investment in servers or software licenses as services such as applications, runtime, data, middleware, operating systems (OS), virtualization, server, storage and networking are managed by the service provider. Hence, a single application is required to be maintained and the cost is lowered. Email and collaboration, customer relationship management, etc. are some examples where Software as a Service (SaaS) model is applied. SaaS is for business users who use services like Email, Office, CRM, Automation etc. for easy completion of business task. A few companies which use SaaS model are Google, Facebook, Sales force, Microsoft, Zoho, etc. [7].

3.2 Platform as a Service (PaaS)

In this model, a cloud provider delivers hardware and software tools usually needed for application development.

The customers use PaaS to build higher levels of service based on PaaS. The customers have the freedom to build their own applications, which run on the provider's infrastructure. While the PaaS provider supports the computing and software like Operating Systems (OS), middleware, virtualization, servers, storage, networking etc. users (or the developer) manages the application only. PaaS providers offer a predefined combination of OS and application servers, such as Linux, Apache, MySQL and PHP (LAMP) platform, restricted J2EE, Ruby etc. to meet manageability and scalability requirements of the applications. PaaS model are used by developers and deployers for testing services, applications, development, integration and deployment. Web sites, web applicationsetc. are some popular fields where PaaS is implemented. Google's App Engine, Force.com, amazon web services are some of the popular services that offer PaaS [7].

3.3 Infrastructure as a Service (IaaS)

IaaS provides basic storage and computing capabilities as standardized services over the network. Servers, storage systems, networking equipment, data centre space etc. are pooled and made available to handle workloads. IaaS is very helpful when the demands in a business are fluctuating, for example there are spikes and downfalls in business demands. IaaS is also useful for start-ups and businesses with very little capital. IaaS is also useful when the business is growing rapidly and scaling hardware would be problematic. It is used by system managers for operating and monitoring services like virtual machines, OS and message queue, network, storage, and CPU etc. Some common technology giants that offer Infrastructure as a Service (IaaS) are Amazon, GoGrid, 3 Tera, Google, OPSource, NTT Communications etc. [7]

4. ADVANTAGES OF CLOUD COMPUTING

Cloud computing has many advantages such as −

Reduced investments and charges- Cloud computing is very cost effective. The single most common economic rationale for investing in cloud-based IT resources is in the reduction or outright elimination of up-front IT investments and ownership costs. It operates at higher efficiencies with much greater utilization. It reduces the investment costs of both hardware and software. It only requires ownership charges. This leads to reduction in the installation cost which is paid by the client at the time of installation.

Easy Accessibility: One can access applications as utilities over the internet.

Easy Installation: It is simple to use and setup all services. It does not require to install specific software to access or manipulate cloud application. The application can be updated at any time without having to worry about resource management and other hassles that come with infrastructure set up and management.

Increased Scalability and Flexibility: Clouds can dynamically allocate IT resources to cloud consumers, on-demand or via the cloud consumer's direct configuration. This enables cloud consumers to scale their cloud-based IT resources to accommodate processing fluctuations and peaks automatically or manually. The service consumers have the flexibility to outsource parts of the infrastructure. It is also flexible for the consumers who wants to swap from capital expenditure to operating expenses.

Increased Availability and Reliability: IT resources are available and accessible for longer periods of time (for example, 22 hours out of a 24-hour day) and by using cloud computing services the client can access their data from anywhere, as and when required. To access the data one needs to login to their account where the data is stored. Cloud providers generally provides resilient IT resources which are easily accessible as utilities over the internet. Due to its modular architecture and load balancing capability cloud environment becomes reliable.

Better Performance: In cloud computing environment user does not need to install heavy software on their own computers. This leads in increasing the performance of the computer.

Unlimited Storage Capacity: With the help of cloud services the client can use the unlimited storage capacity. If the storage requirement of the client increases, client has to pay little more to use a larger storage capacity provided by cloud server. Thus with low installation cost, a user can use unlimited storage capacity.

Maintenance: Cloud service providers do not require applications installations on PCs thus reducing the maintenance cost. In case of natural disaster, the clouds have the backup facility, thus the data can be securely maintained in cloud environment.

Mobile Accessible: As the infrastructure can be accessible from anywhere at any time the number of mobile users have increased.

The availability of high-capacity networks, low-cost computers and storage devices as well as the widespread adoption of hardware virtualization, service-oriented architecture and autonomic and utility computing have led to a growth in cloud computing [8, 9].

5. SECURITY ISSUES IN CLOUD COMPUTING

Cloud computing has mainly two major concerns: namely-security and privacy. Security has been the major concern regarding cloud computing. Security issues such as data loss, phishing, botnet (running remotely on a collection of machines) pose a serious threat to organization's data, software, and in general to the whole cloud system. Hackers can initialize their attack using cloud, by manipulating its structure to fit their needs as it provides more reliable infrastructure at cheaper rates. In the cloud computing world, the virtual environment allows the user to access computing power that exceeds the one that is contained within their physical world. When entering this virtual environment, a user is required to transfer data through the cloud. Consequently, several security concerns arise [10] [11] [12] [13]. Figure 3. Depicts the different data security issues.

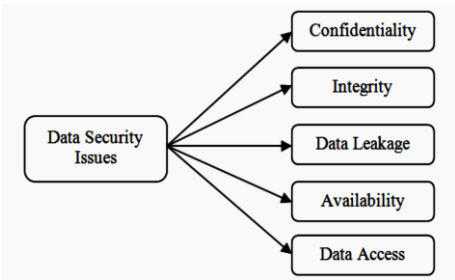

Figure 3. Data security issues

5.1 Computational security

When the computational security over cloud is concerned information security, insecure interfaces and Application Program Interface (API), malicious insider and multi-tenancy play a major role which is explained in detail.

5.1.1 Information security

The data is being stored on the vendor's server so data security is an important issue in the cloud environment. Confidentiality, integrity and security of data is always one of the major concerns and challenges for the SaaS users, regardless of the form of data taken [14]. In SaaS the information is usually processed in plain text and held on within the cloud. The SaaS provider is liable for the safety of the information. Outsourcing is one of the main causes of losing significant control over data.

5.1.2 Insecure interfaces and API

A set of APIs are exposed by the cloud provider to allow its customers to design an interface to manage and interact with cloud service provider. These interfaces make a kind of layer on top of the framework, which in turn, increases the complexity of Cloud [15]. Such stuff allows vulnerabilities in the existing API to continue on its path and ultimately move onto the cloud environment. Furthermore, various organizations and third parties offering cloud-based services often build upon these interfaces to offer value-added services to their customers. This introduces the complexity of the new layered API; it also increases risk. Improper use of such interfaces would often pose threats such as transmission of content, improper authorizations etc. These types of threat may affect the IaaS, PaaS and SaaS service models. The API should be designed to protect against both accidental and malicious attempts to circumvent policy.

5.1.3 Malicious insider

The threat of a malicious insider is well-known to most organizations as there is often little or no visibility into the hiring process of cloud employees. A provider may not reveal how it grants employees access to physical and virtual assets, how to monitor these employees, or how it analyzes and reports on policy compliance. Most of the organizations hide their own policies regarding recruitment procedure of their employees. Due to this kind of situation, the insiders often get a privilege of bypassing the firewall or Intrusion Detection System (IDS), which assumes it to be a legal activity. This kind of situation clearly creates an attractive opportunity for the hobbyist hacker to organize crime. Trusted insider may turn into an adversary by accessing confidential data and gain control over the Cloud services with no risk of detection [16]. This type of threat may be relevant to SaaS, PaaS and IaaS. To avoid this, more transparency is required into security and management process including compliance reporting and breach notification.

5.1.4 Multi-tenancy

In multi-tenant architecture, virtualization is used to offer shared on-demand services. Multi-tenancy is cost effective for SaaS solution providers.

Usually, only three types of virtualization are used:

1. OS level virtualization
2. Application based virtualization
3. Hypervisor based virtualization

In OS level virtualization, multiple guest OSs are running on a hosting OS. Attacker can get control on the entire guest OS(s) by compromising the host OS in this type of configuration. In application based virtualization, virtualization is enabled on the top layer of host OS. Application based virtualization also suffers from same vulnerability as in OS based vulnerabilities. Hypervisor or virtual machine monitor (VMM) which is similar to the code embedded in the host OS. Such code may contain native errors. This code is available during the boot time of the host OS to control multiple guest OS(s). If hypervisor is compromised, then the entire controlled guest OS(s) can be compromised. Vulnerabilities in virtualization or hypervisor allows attacker to perform cross-VM side-channel attacks and DoS attacks.

5.2 Storage security

Having a dynamic hosting environment, cloud suffers the following issues:

5.2.1 Shared technology issues

Cloud vendors deliver their services in a scalable way by sharing infrastructure. But the infrastructure like CPU caches, GPUs, etc. were not designed to offer strong isolation properties for a multi-tenant architecture. To address this gap, a virtualization hypervisor [17] mediates access between the guest operating systems and the physical computer resources. Still even hypervisors cannot take over the control on the underlying platform. Strong compartmentalization should be put into place to ensure that individual customers can neither access to any other tenant's actual or residual data, network traffic nor can create impact in the operations of other tenants running on the same cloud provider.

5.2.2 Data loss and leakage

Deletion or alteration of records without a backup of the original content maybe the most significant reason of compromising with data storage in an unreliable media. The loss of an encoding key may result in unavoidable data destruction. Unauthorized parties may get access to sensitive data which is a big threat in this paradigm. Data losses or leaks can have very severe impacts on a business. The damage to loss of intellectual property is one of the worse cases of data leakage and as a result of malicious attacks, data losses can occur.

5.2.3 Insecure and Ineffective deletion of data

Whenever a provider is changed, resources are scaled down, physical hardware is reallocated, etc., data may be available beyond the lifetime specified in the security policy. It may be impossible to carry out the procedures specified by the security policy, since full data deletion is only possible by destroying a disk, which also may also store data from other clients. When a request to delete a cloud resource is made, this may not result in true wiping of the data (as with most operating systems). Where true data wiping is required, special procedures must be followed and this may not be supported by the standard API (or at all). If effective encryption is used, then the level of risk may be considered to be lower.

5.3. Network security

Cloud computing is vulnerable to various network security issues such as flooding attacks, data interception attacks, management interface attacks, cloud malware attacks and metadata spooling attacks as it uses the internet as the communication media for providing various kinds of different computing services.

5.3.1 Flooding attacks

Cloud computing consists in outsourcing basic operational tasks such as hardware maintenance to a cloud system provider [18]. Thus instead of operating at own internal data center, cloud computing enables users to rent server hardware on demand (IaaS). A user can use these facilities as pay per use process, which provides valuable economic benefits when it comes to dynamics in server load, as for instance, day-and-night cycles can be attenuated by having the data traffic of different time zones operated by the same servers. Instead of buying sufficient server hardware for the high workload times, cloud computing enables a dynamic adaptation of hardware requirements to the actual workload occurring.

5.3.1.1 Direct denial of service

When the cloud computing operating system notices the high workload on the flooded service, it starts to provide more computational power (more virtual machines, more service instances) to cope with the additional workload. The server hardware boundaries for maximum workload to process do no longer hold. In that sense, the cloud system is trying to work against the attacker, but actually to some extent even supports the attacker by enabling him to do most of the possible damage on a service's availability, starting from a single flooding attack entry point. The attacker does not have to flood all servers that provide a certain service in target, but merely can flood a single, cloud-based address in order to perform a full loss of availability on the intended service [18].

5.3.1.2. Indirect denial of service

Depending on the computational power in control of the attacker, a side effect of the direct flooding attack on a cloud service potentially consists in that other services provided on the same hardware servers may suffer from the workload caused by the flooding. If a service instance happens to run on the same server with another, flooded service instance, this may affect its own availability as well. Once the server's hardware resources are completely exhausted by processing the flooding attack requests, obviously also the other service instances on the same hardware machine are no longer able to perform their intended tasks. The denial of service of the targeted service instances are likely to cause a denial of service on all other services deployed to the same server hardware as well. Depending on the level of sophistication of the cloud system, this side-effect may worsen if the cloud system notices the lack of availability, and tries to evacuate the affected service instances to other servers. This results in additional workload for those other servers, and hence the flooding attack jumps over to another service type, and spreads throughout the whole computing cloud. In the worst case, the adversary manages to utilize another (or the very same) cloud computing system for hosting his flooding attack application. In that case, the race in power would play both cloud systems off against each other, each cloud would provide more computational resources for creating, fending the flood until one of them eventually reaches full loss of availability [19].

5.3.2 Data interception attacks:

Cloud computing being a distributed architecture implies more data in transit than traditional infrastructures. The possible reason for data interception attack are sniffing, spoofing, man-in–the-middle attacks, side channel and replay attacks. In some cases, the cloud provider does not offer a confidentiality or non-disclosure clause or these clauses are not sufficient to guarantee protection of the customer's secret information and know-how that will circulate in the cloud [19]. Unauthorized access to resources, difficulty in tracking misuse of resources can happen due to poor system for authentication, authorization of an accounting. Furthermore, the cloud makes password based authentication attacks, since corporate applications are now exposed on the internet. Therefore, password-based authentication becomes insufficient and there is a need for stronger or two-factor authentication while accessing cloud resources. [19].

5.3.3 Management interface attacks

The customer management interfaces of public cloud providers are internet accessible and mediate access to larger sets of resources, thereby posing an increased risk, especially when combined with remote access and web browser vulnerabilities. This includes the customer interfaces controlling the number of virtual machines and most importantly, cloud provider interfaces controlling the operation of the overall cloud system. Of course, this risk may be mitigated by more investment in security by providers [19]. Misconfiguration of specific key parameters of the cloud system is caused due to inadequate application of security baseline or by human error and an untrained administrator.

5.3.4 Cloud malware injection attacks

The main scenario of the cloud malware injection attack is when an attacker uploads a manipulated copy of the intended victim's service instance so that some service requests to the victim service are processed within that malicious instance. These malware attack can destroy the intellectual property of the cloud provider as well as the customers as their confidential data might be stored in the cloud system. The attacker gains control over the victim's data in the cloud system and attempts to retrieve the user credential information and use the same to retrieve critical information from the system. This may degrade the reputation of the cloud service provider.

5.3.5 Metadata spoofing attacks

When an attacker is able to maliciously alter documents, and spread them across web service clients, this attack is called metadata spoofing. When an attacker modifies or changes the service's Web Service Description Language (WSDL) file where descriptions about service instances are stored and succeeds to interrupt service invocation code from WSDL file at delivery time, then such an attack is possible.

6. CONCLUSIONS

Cloud computing is an emerging technology that offers unparalleled distributed computing resources at affordable infrastructure and operating costs. The cloud requires

conscientious and diligent attention from both users and providers due to the inherent risk associated with its operating paradigm. Out of the many obstacles in adopting the cloud model of delivery and consumption of computing resources, security ranks at the top. The lack of strong security controls can resonate through the cloud, opening all of the applications and services that are running across the cloud to exploitation. The internet has changed our lives and its accessibility is essential in day to day services of human life like water, electricity, gas, telephony etc. with ease. So it is high time to address the issues regarding security of the cloud environment. Tremendous amount of work is being done to secure the cloud so that businesses will move to the cloud for the benefits that it offers. With the massive growth in cloud computing adoption, the security attracted the attention of researchers but still it has not been addressed completely. This paper provides a guideline to researcher where they can stand and further identify the issues and enhance cloud-computing security.

ACKNOWLEDGMENT

The authors are sincerely thankful to Prof. (Dr.) Parasar Bandyopadhyay, Director, MCKVIE and Prof. (Dr.) Asok Kumar, Principal, MCKVIE for providing the facilities required for carrying out the said work.

REFERENCES

[1] Rochwerger B., Breitgan, D., Levy E., Galis A., Nagin K., Llorente I.M., Montero R., Wolfsthal Y., Elmroth E., Caceres J., Ben-Yehuda M., Emmerich W., Galan F. (2009). The reservoir model and architecture for open federated cloud computing, *IBM Journal of Research and Development*, Vol. 53, No. 4, pp. 535-545. DOI:10.1147/JRD.2009.5429058

[2] Kyriazis D., Menychtas A., Kousiouris G., Oberle K., Voith T., Boniface M., Oliveros E., Cucinott T., Berger S. (2010). A real-time service oriented infrastructure, *International Conference on Real-Time and Embedded Systems*, Singapore. DOI: 10.5176/9789810876548_R47

[3] Schurr A. (2009). Keep an eye on cloud computing, *Network World*, citing the Gartner report, Cloud Computing Confusion Leads to Opportunity. Retrieved 2009-09-11.

[4] Mohammad H., Ladan T. (2012). Cloud computing uncovered: a research landscape, Elsevier Press, pp. 41-85. ISBN 0-12-396535-7.

[5] Mell P. (2012). What's special about cloud security? *It Professional*, Vol. 14, No. 4, pp. 6-8.

[6] Bandyopadhyay S., Thakur S.S. (2016). Cloud computing: its characteristics, available models, potential challenges and future prospects, *Ipasj International Journal of Information Technology (IIJIT)*, Vol. 4, No. 9, pp. 001-011, ISSN 2321-5976.

[7] Bandyopadhyay S., Thakur S.S. (2016). An overview of cloud computing and cloud service negotiation: some perspectives, *(CCSN 2016)5th International Conference on Computing, Communication and Sensor Network*, pp 106-112.

[8] Cloud Computing: Clash of the clouds, *The Economist*, 2009-10-15.

[9] Gruman G., Knorr E. (2008). What cloud computing really means, InfoWorld, Retrieved 2009-06-02.

[10] George R. (2009). Cloud Application Architectures, First edition, O'Reilly Media, April 2009, ISBN 9780596156367, pp. 2-4, 99-118.

[11] Harauz J., Kaufman L.M., Potter B., Data security in the world of cloud computing, *IEEE Journal on Cloud Computing Security*, Vol. 7, No. 4, pp. 61-64.

[12] Rittinghouse J.W., Ransome J.F. (2009). Cloud computing implementation, management, and security, CRC Press, ISBN 9781439806807, pp. 147-158, 183-212.

[13] Brodkin J. (2008). Gartner: seven cloud-computing security risks, Available: http://www.infoworld.com, pp. 1-3.

[14] Amazon White Paper, http://aws.amazon.com/about-aws/whatsnew/2009/06/08/new-aws-security-center-and-securitywhitepaper/, published June 2009.

[15] Modi C., Patel D., Borisaniya B., Patel A., Rajarajan M. (2013). A survey on security issues and solutions at different layers of cloud computing, *The Journal of Supercomputing*, Vol. 63, No. 2, pp. 561-592. DOI: 10.1007/s11227-012-0831-5

[16] Top 7 threats to cloud computing, HELP NET SECURITY, http://www.net-security.org/secworld.php?id=8943 (2010).

[17] Hypervisor, http://en.wikipedia.org/wiki/Hypervisor

[18] Jensen M., Schwenk J., Gruschka N., Iacono L.L. (2009). On technical security issues in cloud computing, *Proceedings of the 2009 IEEE International Conference on Cloud Computing*, pp. 109-116. DOI: 10.1109/CLOUD.2009.60

[19] Catteddu D. (2010). Cloud computing: benefits, risks and recommendations for information security, Communications in Computer and Information Science, Vol. 72. DOI: 10.1007/978-3-642-16120-9_9